Profile for Use of DisplayName (Draft)

Sampo Kellomäki, Symlabs, Inc.

April 22, 2008

Abstract

Use OrganizationDisplayName as display string for rendering user interfaces and OrganizationURL for indicating a branding image that may be used in the user interfaces.

Document History

01 22. April 2008 Sampo

- Added Background

00 12. February 2008 Sampo Kellomäki (sampo@symlabs.com)

- Proposal

1 Background

The author was engaged by the State Services Commission of the New Zealand Government to advise on the integration of SAML 2.0 into the 'igovt' services offered by this government's Authentication Programme. A number of SAML-related issues arose, based on existing use cases and conceptual designs presented to me. I have taken those issues that I consider to have the greatest implications for the greatest number of real life deployments and proposed solutions for consideration by the SSTC. These are offered with the knowledge and support of the customer, who concluded that, while these issues should be left to deployment, a 'stake in the ground' would help both vendors and implanters alike.

2 Introduction

When presenting user interfaces, a SP often needs to refer to the IdP in a user friendly way, e.g. to present options in IdP selection screen, and conversely, the IdP may occasionally need to refer to the SP in a user friendly way, e.g. to present federation confirmation question.

User friendly presentation usually is a short displayable string that identifies the entity to the users. The string may appear as an option in a popup menu, as an HTML form button, or even as a link. Sometimes a small button image could be used as button or link.

Generally the referred entity (for sake of discussion call this "IdP") cares, for branding reasons, how it is displayed to the users so ideally the referred entity should have some way of conveying the display string or icon to the displaying entity (for sake of discussion call this "SP").

Currently SAML 2.0 has poor facilites for automatically determining or conveying the display string or icon. Most products seem to have local configuration parameters to set the display strings for the members of the Circle of Trust (CoT). This solution has a number of problems:

1. Configuring these options is manual step and as such error prone and costly.
2. Automated CoT construction, e.g. using Well Known Location method of metadata exchange [SAML2meta], p.29, becomes difficult as there is no automatic way to determine the display string or icon. Currently most products appear to try to construct it from the EntityID, but this is suboptimal as EnitytIDs were not necessarily designed to be displayed (neither should there be such constraint on them).
3. If SP administrator configures the display string such that consumers misunderstand what IdP is referred to, the SP administrator may face legal liability.
4. IdP does not get to control its own branding,

Ideally the referred entity (IdP) should decide the display string and icon and be legally responsible for not misleading the consumers. The displaying entity (SP) administrator can in good faith simply display the referred entity branding with disclaimer that the material was provided by the referred entity.

It would seem that the ideal way for IdP to convey its branding to SP (or vice versa) would be via metadata, or the metadata should at least contain a link to where the branding can be obtained in standard form.

Note that the `@ProviderName` in `<AuthnRequest>`, see [SAML2core] section 3.4 "Authentication Request Protocol", p.50, would seem to try to address this issue, but it is an inadequate solution because it only addresses SP presenting its branding to IdP, it is only available in `<AuthnRequest>` interaction, and it lacks localization features or ability to convey an image.

3 Proposal: Use OrganizationDisplayName

SAML metadata [SAML2meta], Section 2.3.2.1 "Element `<Organization>`", p.12, already defines syntax for a number of fields that would seem to suite our needs. However, the actual use of these fields is underspecified. I propose refining the definition of these fields. Each *entity* should be modelled as an `<Organization>`.

The `<OrganizationDisplayName>` SHOULD be human readable name for identifying the entity in user interfaces displayed by other entities that wish to refer to the entity.

`<OrganizationDisplayName>` SHOULD be of such length and formatted in such way, as to allow it to be used in HTML popup lists, selection lists, as button label, or as a link label. In particular, it MUST NOT contain HTML markup, and it SHOULD NOT exceed 40 characters.

In the situations where it is important to identify both the entity and the legal organization that controls or owns it, the `<OrganizationName>` SHOULD identify the controlling or owning organization. While `<OrganizationName>` should be human readable, it SHOULD NOT be used for display or branding purposes in the user interfaces, unless the legal context is relevant.

This approach does not require schema changes. Existing implementations, however, would need to be changed to implement this convention. The change is not foreseen to be difficult, but it is a change.

4 Proposal: Use OrganizationURL for image

The branding image issue is more complicated. The branding image can take several forms

a. Simple image file, such as JPEG or PNG. However, even simple image case needs to deal with potentially multiple sizes of the image.

b. An HTML fragment which may include formatted text or even `<img>` tags. Major problem would be controlling the links that may be embedded in the fragment or the screen real eastate that the fragment tries to grab - not to mention any embedded scripts, etc.

There is also the issue of whether the branding image should be included inline in the metadata, or whether it should be referenced by URL. In the latter case the referenced organization may gain information about accesses to the user interface page that is displayed. Combined with ability to set cookies to one's own domain, quite a lot of information could be gained - or an image customized for the user could be provided.

To simplify matters, I propose that only images of fixed sizes are permitted and that a naming convention is adopted to allow the SP to identify the image size that suites its web page design. These images are referenced using the `<OrganizationURL>` element and thus fetched from the referenced organization (unless cached).

Example metadata fragment

```
  <Organization>
    <OrganizationName>IdP Owner Corp</>
    <OrganizationDisplayName lang="en">Pretty Good IdP</>
    <OrganizationDisplayName lang="pt">IdP razoávelmente boa</>
    <OrganizationURL lang="en">https://pg-idp.com/A/B_saml2_icon_468x60.jpg</>
    <OrganizationURL lang="pt">https://pg-idp.com/C/D_saml2_icon_468x60.jpg</>
    <OrganizationURL lang="en">https://pg-idp.com/A/B_saml2_icon_150x60.png</>
    <OrganizationURL lang="pt">https://pg-idp.com/C/D_saml2_icon_150x60.png</>
    <OrganizationURL lang="en">https://pg-idp.com/A/B_saml2_icon_16x16.gif</>
    <OrganizationURL lang="pt">https://pg-idp.com/C/D_saml2_icon_16x16.gif</>
    <OrganizationURL lang="en">https://pg-idp.com/about.html</>
    <OrganizationURL lang="pt">https://pg-idp.com/sobre.html</>
  </>
```

4.1 Naming convention for branding images

The filename component of the branding image URL MUST match following regular expression

```
  /saml2_icon_(\d+)x(\d+)\.[A-Za-z0-9]+(\?.*)?$/
```

where the first parenthesized number is the width of the image (in pixels) and the second parenthesized number is the hight of the image.

The third parenthesized expression corresponds to an optional Query String component. The filename suffix is not particularly constrained, but should correspond to the customary suffixes used for the image file format. The image file format should be chosen from the widely supported ones, such as JPEG or PNG. The URL prior to filename component and the prefix of the filename component are deliberately left unspecified.

The width and height SHOULD appear in the combinations listed in the Table-1.

Table 1: Branding image sizes

Width	Height	Typical naming
468	60	`B_saml2_icon_468x60.jpg`
150	60	`B_saml2_icon_150x60.jpg`
16	16	`B_saml2_icon_16x16.jpg`

4.2 Algorithm for choosing branding image

The displaying user interface SHOULD use following algorithm to determine which image to display.

1. Select from set of all `<OrganizationURL>`s the ones whose filename component matches the naming convention for any size. This forms a candidate set.

   If this results in empty set, use other means, such as `<OrganizationDisplayName>` for display.

2. Select from the candidate set the ones whose `@lang` XML attribute matches the language of the user interface. If this results in empty set, use implementation dependent heuristic to select next best candidates.

3. Select from the reduced candidate set the first image that matches the desired size. If none match, use implementation dependent heuristic to select the next best candidate, possibly using `@height` and `@width` XML attributes of the `<img>` tag to stretch or shrink the candidate to the desired size.

The selection algorithm and heuristics MUST tolerate `<OrganizationURL>`s that do not follow the naming convention for branding images. Such URLs are valid for other purposes.

The `@lang` XML attribute is optional. If omitted, the treatment is implementation dependent, but every effort SHOULD be made to display something.

5 Discussion

The administrator of the referenced entity (as opposed to who displays the user interface) is legally responsible for correctly representing the referenced entity towards the end user. CoT agreement can further enforce this point, by calling it out and the displayer of the images can insert a disclaimer that it is only displaying material provided by the referenced entity.

The display string is carried inline in the metadata and can, thus, be vetted by displayer according to its policies for accepting metadata.

The branding image is provided by reference and the displayer can not control whether the referenced entity changes the image (possibly after vetting). This provides flexibility, but may be seen by some displayers as a legal threat. They can adopt following solutions:

A. Only use display string

B. Fetch the branding images at the time of vetting and store them locally (this may require copyright license clause to be inserted into the CoT agreement). When displaying, point to the local copies. This technique also avoids leaking traffic analysis information to the referenced entity and prevents the cookie related abuse or personalization.

It is intentional that the mapping between display representation of an entity and its EntityID is not necessarily one-to-one. If a commercial company operates an affiliation of entities, it may be completely acceptable that they are identified by the same display string and branding, as long as the user is not misled.

5.1 Minimal change vs. extension

Another possible way to solve the display string and branding image problem would be to extend the metadata schema to explicitly express them. We felt that the product cycles would mean that solution would become available much later than with the present scheme.

Normative

[SAML2core] "Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0", Oasis Standard, 15.3.2005, saml-core-2.0-os

[SAML2prof] "Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0", Oasis Standard, 15.3.2005, saml-profiles-2.0-os

[SAML2bind] "Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0", Oasis Standard, 15.3.2005, saml-bindings-2.0-os

[SAML2context] "Authentication Context for the OASIS Security Assertion Markup Language (SAML) V2.0", Oasis Standard, 15.3.2005, saml-authn-context-2.0-os

[SAML2meta] Cantor, Moreh, Phipott, Maler, eds., "Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0", Oasis Standard, 15.3.2005, saml-metadata-2.0-os

[SAML2security] "Security and Privacy Considerations for the OASIS Security Assertion Markup Language (SAML) V2.0", Oasis Standard, 15.3.2005, saml-sec-consider-2.0-os

[SAML2conf] "Conformance Requirements for the OASIS Security Assertion Markup Language (SAML) V2.0", Oasis Standard, 15.3.2005, saml-conformance-2.0-os

[SAML2glossary] "Glossary for the OASIS Security Assertion Markup Language (SAML) V2.0", Oasis Standard, 15.3.2005, saml-glossary-2.0-os

[IDFF12] http://www.projectliberty.org/resources/specifications.php

[IDFF12meta] Peted Davis, Ed., "Liberty Metadata Description and Discovery Specification", version 1.1, Liberty Alliance Project, 2004. (liberty-metadata-v1.1.pdf)

[RFC2119] Bradner, S., "Key Words for use in RFCs to Indicate Requirement Levels," BCP 14, RFC 2119, March 1997.

[Schema1-2] Henry S. Thompson et al. (eds): XML Schema Part 1: Structures, 2nd Ed., WSC Recommendation, 28. Oct. 2004, http://www.w3.org/2002/XMLSchema